IV&V Methodologies and Effectiveness with Small IV&V Teams

July 19th 2004

At NASA IV&V Facility
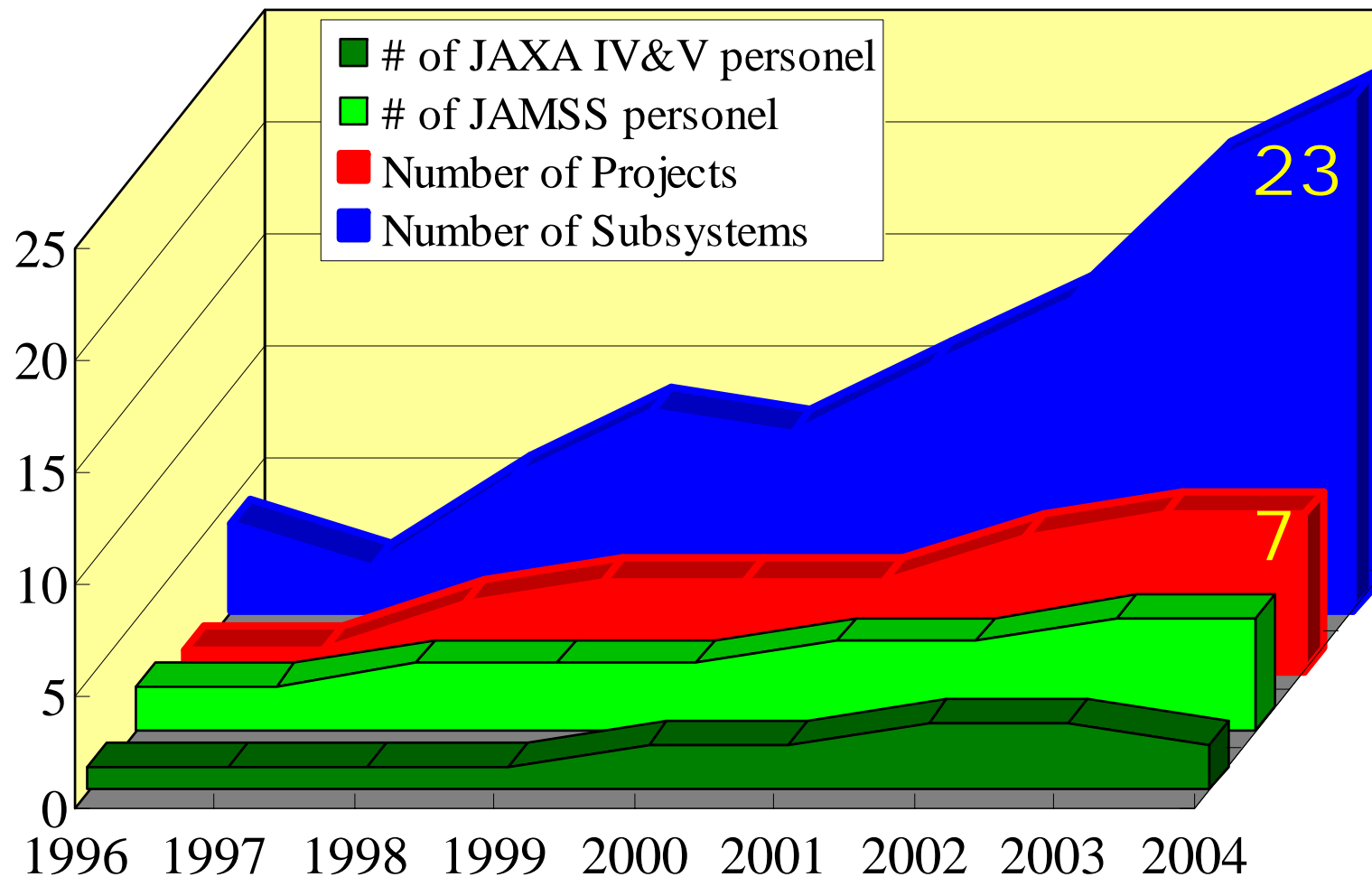
Masa Katahira

Information Technology Center

Japan Aerospace Exploration Agency (JAXA)

Objectives of Software IV&V in JAXA

- Projects' software development evaluation

- Research of new software engineering methodologies

- Introducing those methodologies into development team and contractors

Increasing S/W IV&V applied Projects

Methodology Selection

Small Budget →

Short Period of IV&V →

Check List Base / Model Checking & Simulation (full set)

← Proper Budget

← Proper Period of IV&V

Small Team →

Design Data Access Limitation →

Team supported By development contractor / Pure Independent Team

← Proper Team size

Organization Selection

Checklist Sample
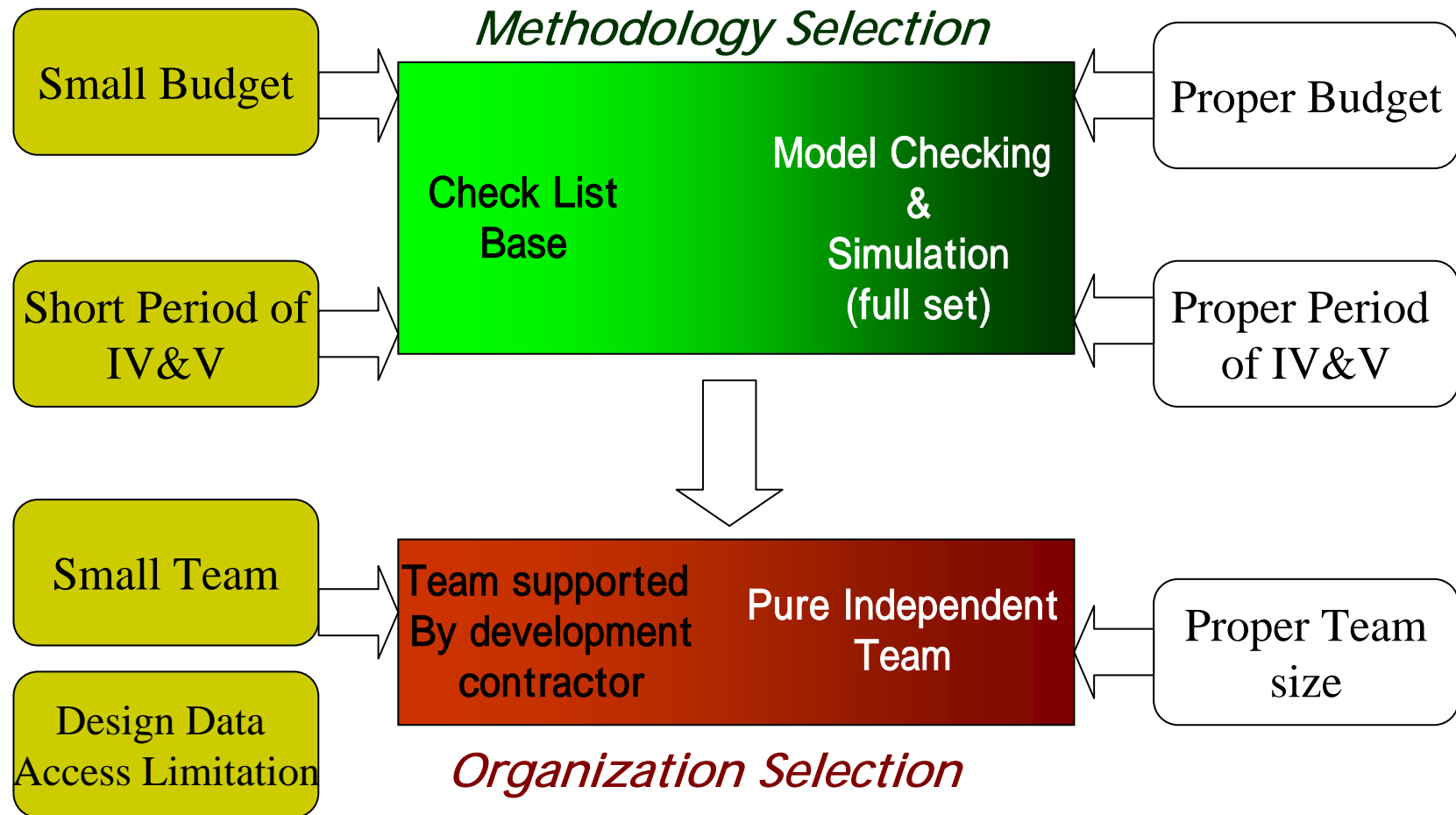
■ **Lessons Learnt base checklist**

  ◎ Study from past accidents and problems

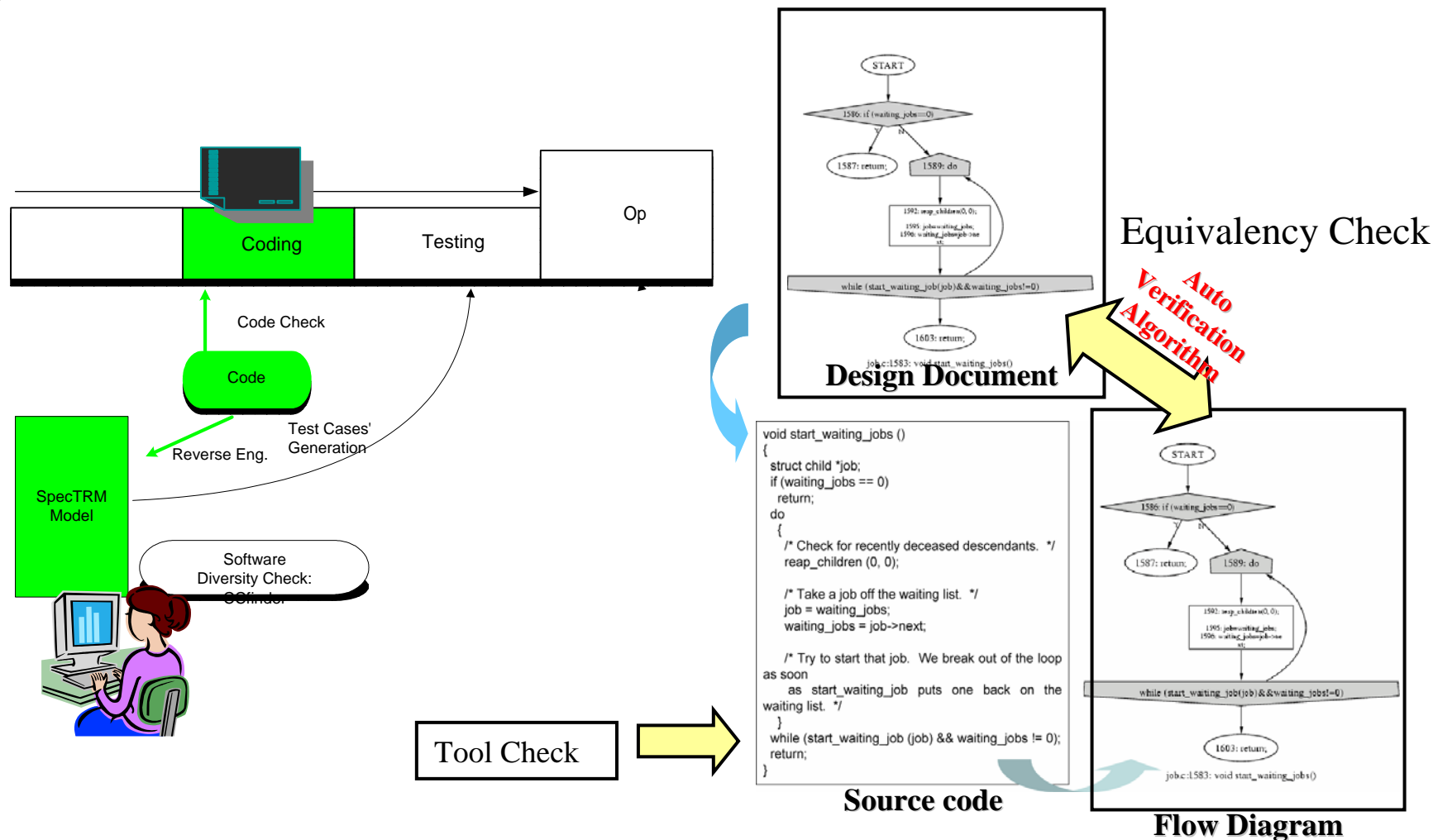 ◎ Interview of experienced engineers

■ **e.g.**

  "Satellite Attitude Control Software Check list": more than 200 detailed concrete check items

Check Item	Points	Document to be reviewed	Priority	Difficulty
Is there mistake of detection direction/+ - of Roll/Pitch?	There were many cases to mistake +/- of roll/pitch angle from earth sensors, especially when main and redundant sensors' position and aliment was different.	Interface definition document software requirement specification	high	high

Full set of IV&V Methodologies

Sample of Model based Approach

Specification

AA Mode

A) The SYSTEM XYZ shall (REQ-01001) transfer mode from **every mode without Initialization Mode or B Mode** to AA Mode by command.

Documents(Flow)

Modeling

SpecTRM

> Completeness
> Consistency
> Traceability
> Equivalency
> Reachability
> Interface check

Natural Language Model (SpecTRM Model)

AA Mode (REQ-01001)
'XYZ is Stanby_Mode' and 'AA_Mode_Command is ON'
Or 'XYZ is AA_Mode' and 'AA_Mode_Command is ON'
Or 'XYZ is AB_Mode' and 'AA_Mode_Command is ON'
=> XYZ is AA_Mode

Auto code generation to C ⇨ Executable model ⇨

Simulation
Unreachable flow
Inconsistency branch

Traceability and Equivalen

Op

Coding

Testing

Code Check

Code

Reverse Eng.

Test Cases' Generation

SpecTRM Model

Software Diversity Check: CCfinder

Equivalency Check

Auto Verification Algorithm

Design Document

Source code

```
void start_waiting_jobs ()
{
  struct child *job;
  if (waiting_jobs == 0)
    return;
  do
    {
      /* Check for recently deceased descendants.  */
      reap_children (0, 0);

      /* Take a job off the waiting list.  */
      job = waiting_jobs;
      waiting_jobs = job->next;

      /* Try to start that job.  We break out of the loop
as soon
        as start_waiting_job puts one back on the
waiting list.  */
    }
  while (start_waiting_job (job) && waiting_jobs != 0);
  return;
}
```
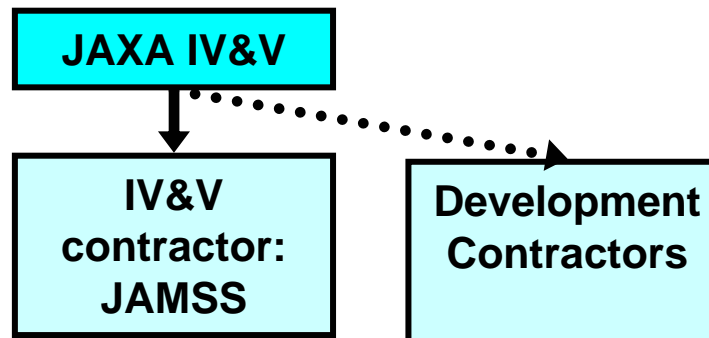
Flow Diagram

Tool Check

IV&V team sizing

■ Pure Independent Team   ■ Small Team

JAXA IV&V

IV&V contractor: JAMSS

IV&V sub-contractor

JAXA IV&V

IV&V contractor: JAMSS

Development Contractors

JAXA IV&V

■ Other cases

JAXA Development Team

IV&V contractor: JAMSS

JAXA Development Team

Development Contractors